





DE10020563

Patent number: DE10020563
Publication date: 2001-04-19
Inventor: LANG JUERGEN (DE); MEYER BERND (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
- **international:** *H04L9/32; H04L9/32; (IPC1-7): H04L9/32*
- **european:** H04L9/32
Application number: DE20001020563 20000427
Priority number(s): DE20001020563 20000427; DE19991048319 19991007

Also published as:

 WO0125880 (A3)
 WO0125880 (A2)
 CA2425184 (A1)
 AU773985 (B2)

Report a data error here

Abstract of DE10020563

The invention relates to a method for producing forge-proof documents using a security module, whereby the security module generates a temporary secret which is unknown to the document producer. The temporary secret, in conjunction with information revealed about the identity of the security module, is transferred in encrypted form to an authentication unit. Said authentication unit decodes the temporary secret, recognizes the identity of the security module and the temporary secret together with other information which is coded in such a way that only one checking station can implement decoding and transfer said temporary secret to the document producer. The document producer transfers producer data, which is integrated into the document, to the security module. The data introduced into the security module by said document producer is irreversibly linked with the temporary secret in such a way that repeated linking of the same data in the same manner yields an identical result. It is not possible to draw conclusions about the temporary secret. The inventive method is characterized in that the result of the irreversible linking of data introduced by said document producer can be introduced into said document together with said temporary secret. The invention also relates to a method for checking the authenticity of a given document.

Data supplied from the **esp@cenet** database - Worldwide

19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

12 **Offenlegungsschrift**
10 **DE 100 20 563 A 1**

51 Int. Cl.⁷:
H 04 L 9/32

21 Aktenzeichen: 100 20 563.1
22 Anmeldetag: 27. 4. 2000
43 Offenlegungstag: 19. 4. 2001

DE 100 20 563 A 1

66 Innere Priorität:

199 48 319. 1 07. 10. 1999

71 Anmelder:

Deutsche Post AG, 53175 Bonn, DE

74 Vertreter:

Jostarndt Thul Patentanwälte, 52076 Aachen

72 Erfinder:

Lang, Jürgen, Dr., 51429 Bergisch Gladbach, DE;
Meyer, Bernd, 53639 Königswinter, DE

56 Entgegenhaltungen:

DE	197 03 929 A1
DE	195 13 896 A1
US	58 72 848
EP	8 87 997 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Verfahren zur Erstellung und Überprüfung fälschungssicherer Dokumente

57 Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls, wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt, wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird, wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und an den Dokumenthersteller übermittelt, wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt, wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind.

Erfindungsgemäß zeichnet sich dieses Verfahren dadurch aus, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis in das Dokument übernommen wird.

Die Erfindung betrifft ferner ein Verfahren zur Überprüfung der Echtheit eines Dokuments.

DE 100 20 563 A 1

Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls, wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt, wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird, wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und das verschlüsselte temporäre Geheimnis und die weiteren Informationen an den Dokumenthersteller übermittelt, wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt, wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind.

Die Erfindung betrifft ferner ein Verfahren zur Überprüfung der Echtheit eines Dokuments.

An diesem Verfahren und diesem System, die die Funktionsweisen eines Sicherungsmoduls im Umfeld der digitalen Signatur und des Einsatzes von Verschlüsselungstechniken betreffen, sind neben dem Sicherungsmodul drei Parteien beteiligt:

- der Hersteller/Bearbeiter eines Dokuments, nachfolgend "Dokumenthersteller" genannt,
- eine Bescheinigungsstelle, die das Sicherungsmodul identifizieren und mit der Identität des Dokumentherstellers verknüpfen kann und
- eine Prüfstelle, bei der die Prüfungen der Unverfälschtheit des Dokuments und der Identität des Dokumentherstellers stattfindet.

Zur Gewährleistung der Fälschungssicherheit von Dokumenten und zur Identifizierung von Dokumentherstellern sind Systeme zur digitalen Signatur wie etwa Public-Key-Signaturverfahren nach Patentschrift DE 195 13 896 A1 oder DE 197 03 929 A1 bekannt.

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vgl. SigG § 2, Abs. 1). Unter Benutzung der hier verwandten Terminologie ist eine Prüfstelle in der Lage, die digitale Signatur eines Dokumentherstellers und somit sowohl dessen Identität als auch die Unverfälschtheit der im Dokument enthaltenen Daten zu prüfen, wenn ihr der öffentliche Signaturschlüssel des Dokumentherstellers, der mit einem Signaturschlüssel-Zertifikat versehen ist, zur Verfügung steht.

Problematisch ist die Anwendung des Verfahrens der digitalen Signatur dann, wenn entweder der Prüfstelle nicht der öffentliche Signaturschlüssel des Dokumentherstellers, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, zur Verfügung steht oder der Dokumenthersteller keinen eigenen privaten oder öffentlichen Signaturschlüssel besitzt.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren

zur Erstellung und/oder Überprüfung fälschungssicherer Dokumente zu schaffen, das auch dann einsetzbar ist, wenn die Prüfstelle nicht den öffentlichen Signaturschlüssel des Dokumentherstellers kennt und/oder wenn der Dokumenthersteller keinen eigenen privaten oder öffentlichen Signaturschlüssel besitzt.

Erfindungsgemäss wird diese Aufgabe dadurch gelöst, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis in das Dokument übernommen wird.

Gegenstand der Erfindung ist ferner, ein gattungsgemäßes Verfahren zum Überprüfen der Echtheit von Dokumenten so durchzuführen, dass die Prüfungsstelle überprüft, ob ein Ergebnis einer irreversiblen Verknüpfung aus von einem Dokumenthersteller eingebrachten Daten und einem Geheimnis in das Dokument übernommen wurde, indem die Prüfstelle das Geheimnis und weitere Informationen, die von einer Bescheinigungsstelle verschlüsselt wurden, entschlüsselt.

Hierbei ist es besonders vorteilhaft, dass die Prüfstelle in derselben Weise wie ein zur Herstellung des fälschungssicheren Dokuments eingesetztes Sicherungsmodul die von dem Dokumenthersteller in das Dokument eingebrachten Daten mit dem entschlüsselten temporären Geheimnis irreversibel verknüpft.

Zur Erhöhung der Datensicherheit bei der Erstellung der Dokumente ist es zweckmäßig, das Verfahren zur Erstellung der Dokumente so durchzuführen, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden.

Hierbei ist es besonders vorteilhaft, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen, die neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden, derart übermittelt werden, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann.

Zweckmässigerweise wird das Verfahren so durchgeführt, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen Angaben zur Identität des Dokumentherstellers und zur Gültigkeit der von dem Dokumenthersteller hergestellten Dokumente enthält.

Um zu überprüfen, ob die Dokumente nach dem zuvor beschriebenen Verfahren von dem dazu berechtigten Dokumenthersteller erzeugt wurden, ist es zweckmäßig, das Verfahren zur Überprüfung der Echtheit des Dokuments so durchzuführen, dass die Prüfstelle das Ergebnis der selbst durchgeführten irreversiblen Verknüpfung mit einem Ergebnis einer von dem Dokumenthersteller durchgeführten irreversiblen Verknüpfung vergleicht, die in das Dokument übernommen wurde.

Hierbei ist es vorteilhaft, dass durch den Vergleich ermittelt wird, ob in das Dokument von dem Dokumenthersteller eingebrachte Daten verfälscht wurden.

Obwohl die Schritte des Herstellens und des Prüfens voneinander getrennt stattfinden, ist eine Verbindung zu einem Gesamtverfahren, bei dem sowohl die Erzeugung als auch die Prüfung der Dokumente nach zuvor festgelegten Kriterien erfolgen, besonders vorteilhaft.

Hierbei ist es zweckmäßig, dass keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen der Bescheinigungs- und der Prüfstelle stattfindet.

Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung eines bevorzugten Ausführungsbeispiels anhand der Zeichnungen.

Von den Zeichnungen zeigt

Fig. 1 ein Sicherungsmodul, das in dem Verfahren eingesetzt werden kann und

Fig. 2 eine schematische Darstellung eines Systems zur Erzeugung und zur Überprüfung fälschungssicherer Dokumente.

Durch das hier beschriebene Verfahren und System ergibt sich für eine Prüfstelle, bei der der Dokumenthersteller und das von ihm hergestellte Dokument nicht bekannt sind, die Möglichkeit, auch ohne Anwendung der digitalen Signatur durch den Dokumenthersteller die Unverfälschtheit der in dem Dokument enthaltenen Daten sowie der Identität des Dokumentherstellers zuverlässig zu prüfen.

Hierzu verwendet der Dokumenthersteller ein Sicherungsmodul, das unter Einsatz unterschiedlicher technischer Mittel, vorzugsweise unter Zusammenwirken von Software mit programmierbarer Hardware realisiert wird und 5 aktive und 3 passive Einheiten sowie 2 Datenausgänge und 1 Dateneingang enthält (vgl. Zeichnung 1).

Die aktiven Einheiten sind:

- ein Geheimnisgenerator, der ein nicht vorhersagbares, temporäres Geheimnis erzeugt (Zufallszahl),
- eine Verschlüsselungsmaschine, die nach bekannten Verfahren einen Eingangswert mit einem in einem Register gespeicherten Schlüssel verschlüsselt,
- eine Hash-Maschine, die nach einem bekannten Verfahren aus einem Eingangswert einen Hash-Wert dieses Eingangswerts bildet (vgl. SigV § 17, Abs. 2) und
- zwei Kombinationsmaschinen, die aus jeweils zwei Eingangswerten einen Ergebniswert zusammensetzen.

Die passiven Einheiten sind:

- ein Schlüsselregister, in dem ein Schlüssel gespeichert ist, mit dem Verschlüsselungen erzeugt werden können, die nur von der Bestätigungsstelle entschlüsselt werden können,
- ein Identifikationsregister, in dem Dateien enthalten sind, mit denen sich das Sicherungsmodul bei einer Bestätigungsstelle eindeutig identifizieren kann und
- ein Zwischenspeicher, in dem das im Geheimnisgenerator erzeugte Geheimnis temporär gespeichert wird.

Die Dateneingänge und die Datenausgänge sind die einzigen richtungsspezifischen Eingabe- und Ausgabemöglichkeiten für das Sicherungsmodul. Eine andere Art des Zugriffs oder Zugangs zum Sicherungsmodul ist weder für den Dokumenthersteller noch für Dritte möglich. Im Einzelnen handelt es sich bei den Dateneingängen und Datenausgängen um:

- einen Datenausgang 1, durch den Daten ausgegeben werden, die an die Bescheinigungsstelle übertragen werden,
- einen Datenausgang 2, durch den Daten ausgegeben werden, die auf das Dokument übernommen werden und
- einen Dateneingang, durch den Informationen vom Dokumenthersteller in das Sicherungsmodul eingegeben werden können.

Vorzugsweise wird in dem Verfahren zur Erstellung der fälschungssicheren Dokumente das nachfolgend dargestellte Sicherungsmodul eingesetzt.

In dem Sicherungsmodul erzeugt ein Geheimnisgenerator ein nicht vorhersagbares Geheimnis (zum Beispiel eine Zufallszahl), das außerhalb des Sicherungsmoduls unbekannt bleibt, und übergibt dieses Geheimnis einerseits an die

Kombinationsmaschine 1 und andererseits an den Zwischenspeicher. Die Kombinationsmaschine 1 kombiniert das Geheimnis mit den im Identifikationsregister enthaltenen Daten, die das Sicherungsmodul bei einer Bestätigungsstelle eindeutig identifizieren. Der Ergebniswert der Kombinationsmaschine wird in die Verschlüsselungsmaschine eingegeben, die mit dem Schlüssel aus dem Schlüsselregister einen verschlüsselten Ergebniswert erzeugt, der nur von der Bescheinigungsstelle entschlüsselt werden kann. Dieser Ergebniswert wird aus dem Datenausgang 1 aus dem Sicherungsmodul ausgegeben, um an die Bescheinigungsstelle übertragen zu werden.

Entschlüsselt die Bescheinigungsstelle den aus Datenausgang 1 ausgelassenen und übertragenen Ergebniswert, zerlegt sie diesen Ergebniswert in das Geheimnis und die Daten aus dem Identifikationsregister, identifiziert das Sicherungsmodul anhand der Daten aus dem Identifikationsregister und verschlüsselt das Geheimnis und weitere Informationen mit einem Schlüssel, der nur von der Prüfstelle entschlüsselt werden kann, so können das verschlüsselte Geheimnis und weitere Informationen an den Dokumenthersteller übertragen, von diesem auf das Dokument übernommen und von der Prüfstelle entschlüsselt werden.

Daten, die der Dokumenthersteller selbst über den Dateneingang in das Sicherungsmodul einbringt, werden von der Kombinationsmaschine 2 mit dem im Zwischenspeicher gespeicherten Geheimnis kombiniert. Der Ergebniswert der Kombinationsmaschine 2 wird in die Hash-Maschine eingegeben, die nach einem bekannten Verfahren einen Hash-Wert des eingegebenen Wertes bildet. Dieser Ergebniswert wird aus dem Datenausgang 2 aus dem Sicherungsmodul ausgegeben, um in das Dokument übernommen zu werden.

In das Dokument übernommen werden vorzugsweise:

- diejenigen Daten, die der Dokumenthersteller selbst über den Dateneingang in das Sicherungsmodul eingebracht hat,
- der durch Datenausgang 2 aus dem Sicherungsmodul ausgegebene Hash-Wert und
- das von der Bescheinigungsstelle verschlüsselte Geheimnis und weitere Informationen, die nur von der Prüfstelle entschlüsselt werden können.

Eine Prüfstelle führt die Prüfung der Unverfälschtheit des Dokuments und der Identität des Dokumentherstellers durch, indem das von der Bescheinigungsstelle verschlüsselte Geheimnis und weitere Informationen entschlüsselt werden, nach einem bekannten Verfahren ebenso wie im Sicherungsmodul ein Hash-Wert aus einer Kombination aus den vom Dokumenthersteller selbst eingebrachten Daten und dem Geheimnis gebildet wird und dieser Hash-Wert mit dem übermittelten Hash-Wert verglichen wird. Ergibt der Vergleich der Hash-Werte – analog zur Prüfung einer digitalen Signatur – eine Identität des erzeugten und des übermittelten Hash-Wertes, so kann das Dokument nicht verfälscht worden sein.

Von der Bescheinigungsstelle werden weitere Informationen derart verschlüsselt an den Dokumenthersteller übermittelt, dass nur die Prüfstelle sie entschlüsseln kann, und die an den Dokumenthersteller zur Übernahme in das fälschungssichere Dokument übermittelt werden, um Informationen zur Identität des Dokumentherstellers und zum Gültigkeitszeitraum der vom Dokumenthersteller hergestellten Dokumente.

Ein bevorzugtes Einsatzgebiet der Erfindung besteht darin, dass Dokumenthersteller beispielsweise solche Personen sind, die über einen Computer (PC) Dokumente wie beispielsweise Eintrittskarten, Flugtickets oder Gutscheine

selbst ausdrucken, deren Unverfälschtheit von einer Prüfstelle, die beispielsweise den entsprechenden Eintritt regelt, verifiziert werden kann. Die Bescheinigungsstelle ist beispielsweise die Ausgabestelle der Eintrittskarten, mit der der Dokumenthersteller im Vorfeld des Ausdrucks der Eintrittskarten auf elektronischem Weg über das Internet kommuniziert. Das Sicherungsmodul ist ein technisches Mittel, das vorzugsweise unter Zusammenwirken von Software mit programmierbarer Hardware realisiert wird und zumindest temporär Bestandteil der Hard- und Software des PC des Dokumentherstellers ist.

Die Erfindung kann sicherstellen, dass beispielsweise die den Eintritt regelnde Prüfstelle auch ohne Prüfung der digitalen Signatur des Dokumentherstellers mit all den hieraus erwachsenen Konsequenzen (individuelle öffentliche Signaturschlüssel aller zu prüfenden Dokumenthersteller) die Unverfälschtheit eines Dokuments verifizieren kann, das im Einflußbereich eines nicht vertrauenswürdigen Dokumentherstellers über dessen PC und Drucker erstellt wurde. Das Sicherungsmodul gewährleistet dabei die Unverfälschbarkeit von Informationen, die vom Dokumenthersteller ohne Kenntnis der Bescheinigungsstelle in das Dokument eingefügt wurden, sowie die Identifizierbarkeit des Dokumentherstellers.

Vorteilhafte Wirkungen dieser Erfindung sind darin zu sehen, dass Firmen und Organisationen ihren Kunden durch den Einsatz von Sicherungsmodulen die Möglichkeit geben können, einfach über das Internet den Ausdruck von Dokumenten zu erlauben, deren Unverfälschtheit zweifelsfrei geprüft werden kann. Besonders vorteilhaft ist hierbei der Verzicht auf den Einsatz digitaler Signaturen durch den Dokumenthersteller, der mit einem erheblichen infrastrukturellen, organisatorischen Aufwand und einer landesspezifischen Rechtsunsicherheit einhergeht. Weiterhin ist es bei dem beschriebenen Verfahren und System vorteilhaft, dass der Umfang derjenigen Informationen, die innerhalb des Dokuments der Prüfung durch die Prüfstelle dienen, im Vergleich zur digitalen Signatur, bei der der öffentliche, mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehene Signaturschlüssel des Dokumentherstellers einen Teil des Dokuments darstellen kann, sehr gering ist. Vorteilhaft ist weiterhin, dass zur Prüfung der Unverfälschtheit keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen Bescheinigungs- und Prüfstelle stattfinden muss. Vorteilhaft ist schließlich, dass eine grundsätzliche Entkopplung zwischen der Kommunikation zwischen dem Sicherungsmodul und der Bescheinigungsstelle einerseits und der Dokumentherstellung und -prüfung andererseits in der Art erfolgen kann, dass mehrere Dokumente auf Basis einer Kommunikation zwischen Sicherungsmodul und Bescheinigungsstelle hergestellt werden können, in die vom Dokumenthersteller unterschiedliche dokumentspezifische Daten eingegeben werden können.

Ein zweckmässiges Verfahren zur Erzeugung und Prüfung fälschungssicherer Dokumente wird nachfolgend anhand von Fig. 2 dargestellt.

In Fig. 2 ist ein System dargestellt, in dem von einem Dokumenthersteller erzeugte Informationen an eine Bescheinigungsstelle übertragen, dort verarbeitet und erneut an den Dokumenthersteller übertragen werden. Der Dokumenthersteller stellt unter Verwendung der von der Bescheinigungsstelle übermittelten Informationen fälschungssichere Dokumente her. Ein von der Dokumentherstellung vorzugsweise getrennter Vorgang ist eine Prüfung der fälschungssicheren Dokumente in einer Prüfstelle.

Das dargestellte System beinhaltet die nachfolgend dargestellten Prozessschritte 1 bis 8.

In einem ersten Prozessschritt 1 erfolgt die Erzeugung eines temporären Geheimnisses in Form einer Zufallszahl, die zusammen mit einer Identifikationsnummer des Sicherungsmoduls mit dem öffentlichen Schlüssel der Bescheinigungsstelle verschlüsselt wird, so dass dieses temporäre Geheimnis dem Dokumenthersteller nicht zur Kenntnis gelangen kann und nur von der Bescheinigungsstelle entschlüsselt werden kann.

In dem mit dem Bezugszeichen 2 gekennzeichneten Prozessschritt erfolgt die Übertragung der verschlüsselten Zufallszahl und Identifikationsnummer zur Bescheinigungsstelle. Zu beachten ist, dass diese Übertragung auch über einen unsicheren Weg vonstatten gehen kann, da nur die Bescheinigungsstelle in der Lage ist, die Informationen zu entschlüsseln.

In einem anschließenden Verfahrensschritt 3 erfolgt in der Bescheinigungsstelle die Entschlüsselung der Zufallszahl und der Identifikationsnummer mit dem privaten Schlüssel der Bescheinigungsstelle. Die Zufallszahl wird mit weiteren Informationen zur Identität des Dokumentherstellers zum Gültigkeitszeitraum der vom Dokumenthersteller hergestellten Dokumente derart verschlüsselt, dass nur die Prüfstelle die Zufallszahl und die weiteren Informationen entschlüsseln kann.

In dem mit dem Bezugszeichen 4 gekennzeichneten Verfahrensschritt erfolgt eine Übertragung der verschlüsselten Informationen zum Dokumenthersteller. Zu beachten ist, dass diese Übertragung auch über einen unsicheren Weg vonstatten gehen kann, da nur die Prüfstelle in der Lage sein wird, die Informationen zu entschlüsseln.

Aus diesem Grund eignet sich das Verfahren besonders für einen Einsatz in Datennetzen, die als solche gegen einen unbefugten Zugang nicht oder nur schwer gesichert werden können, wie dem Internet.

In dem mit dem Bezugszeichen 5 gekennzeichneten Verfahrensschritt gibt der Dokumenthersteller in das Sicherungsmodul eigene Daten ein, die zu einer Kennzeichnung des Dokuments dienen.

In dem mit dem Bezugszeichen 6 gekennzeichneten Verfahrensschritt erfolgt eine Bildung eines Hash-Wertes aus der Kombination von dem Dokumenthersteller eingegebenen Daten und der noch gespeicherten Zufallszahl. Das anschließend hergestellte Dokument enthält die Daten, die der Dokumenthersteller selbst in das Dokument einbringt, den soeben gebildeten Hash-Wert sowie die verschlüsselten Informationen der Bescheinigungsstelle.

In einem weiteren Verfahrensschritt 7 erfolgt eine Übertragung des Dokuments, das aus den Daten des Benutzers, dem Hash-Wert und den verschlüsselten Informationen der Bescheinigungsstelle (vgl. Ziffer 3) besteht.

In einer Prüfstelle erfolgt in einem mit dem Bezugszeichen 8 gekennzeichneten Verfahrensschritt eine Entschlüsselung der Informationen der Bescheinigungsstelle mit dem Schlüssel der Prüfstelle. Nach Patentanspruch 1 kann die entschlüsselte Zufallszahl benutzt werden, um zusammen mit den Daten, die der Dokumenthersteller selbst in das Dokument eingebracht hat, einen Hash-Wert nach demselben, bekannten Verfahren zu bilden, das im Sicherungsmodul zur Bildung des Hash-Wertes benutzt wurde. Ein Vergleich des gebildeten Hash-Wertes mit dem übertragenen Hash-Wert gibt zuverlässige Auskunft darüber, ob die vom Dokumenthersteller selbst eingebrachten Daten verfälscht wurden. Nach Patentanspruch 2 können hierbei weitere Informationen zur Identität des Dokumentherstellers und zum Gültigkeitszeitraum der vom Dokumenthersteller hergestellten Dokumente entschlüsselt werden.

Durch das Verfahren und System zur Erstellung fälschungssicherer Dokumente unter Benutzung eines Siche-

rungsmoduls ergibt sich für eine Prüfstelle, bei der ein Dokumenthersteller und das von ihm hergestellte Dokument nicht bekannt sind, die Möglichkeit, auch ohne Anwendung der digitalen Signatur durch den Dokumenthersteller die Unverfälschtheit der in dem Dokument enthaltenen Daten sowie die Identität des Dokumentherstellers zuverlässig zu prüfen. Alle hierzu erforderlichen Prüfinformationen, die in das Dokument zu übernehmen sind, werden von einer Bescheinigungsstelle zur Verfügung gestellt, mit der das beim Dokumenthersteller betriebene Sicherungsmodul im Vorfeld der Herstellung/Bearbeitung des Dokuments kommuniziert. Das Verfahren und System eignet sich insbesondere, um Personen die Möglichkeit zu geben, beispielsweise Eintrittskarten oder Gutscheine über den eigenen PC auszudrucken, die zweifelsfrei auf Unverfälschtheit geprüft werden können.

Patentansprüche

1. Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls,
 - wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt,
 - wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird,
 - wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und das temporäre Geheimnis und die weiteren Informationen an den Dokumenthersteller übermittelt,
 - wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt,
 - wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und
 - wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind,
 dadurch gekennzeichnet, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis in das Dokument übernommen wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen, die neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden, derart übermittelt werden, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann.
4. Verfahren nach einem oder mehreren der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen Angaben zur Identität des Dokumentherstellers und zur Gültigkeit der von dem Doku-

menthersteller hergestellten Dokumente enthält.

5. Verfahren zur Überprüfung der Echtheit eines Dokuments, dadurch gekennzeichnet, dass die Prüfstelle überprüft, ob ein Ergebnis einer irreversiblen Verknüpfung aus von einem Dokumenthersteller eingebrachten Daten und einem Geheimnis in das Dokument übernommen wurde, indem die Prüfstelle das Geheimnis und weitere Informationen, die von einer Bescheinigungsstelle verschlüsselt wurden, entschlüsselt, und dass die Prüfstelle in derselben Weise wie ein zur Herstellung des fälschungssicheren Dokuments eingesetztes Sicherungsmodul die von dem Dokumenthersteller in das Dokument eingebrachten Daten mit dem entschlüsselten temporären Geheimnis irreversibel verknüpft.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die Prüfstelle das Ergebnis der selbst durchgeführten irreversiblen Verknüpfung mit einem Ergebnis einer von dem Dokumenthersteller durchgeführten irreversiblen Verknüpfung vergleicht, die in das Dokument übernommen wurde.

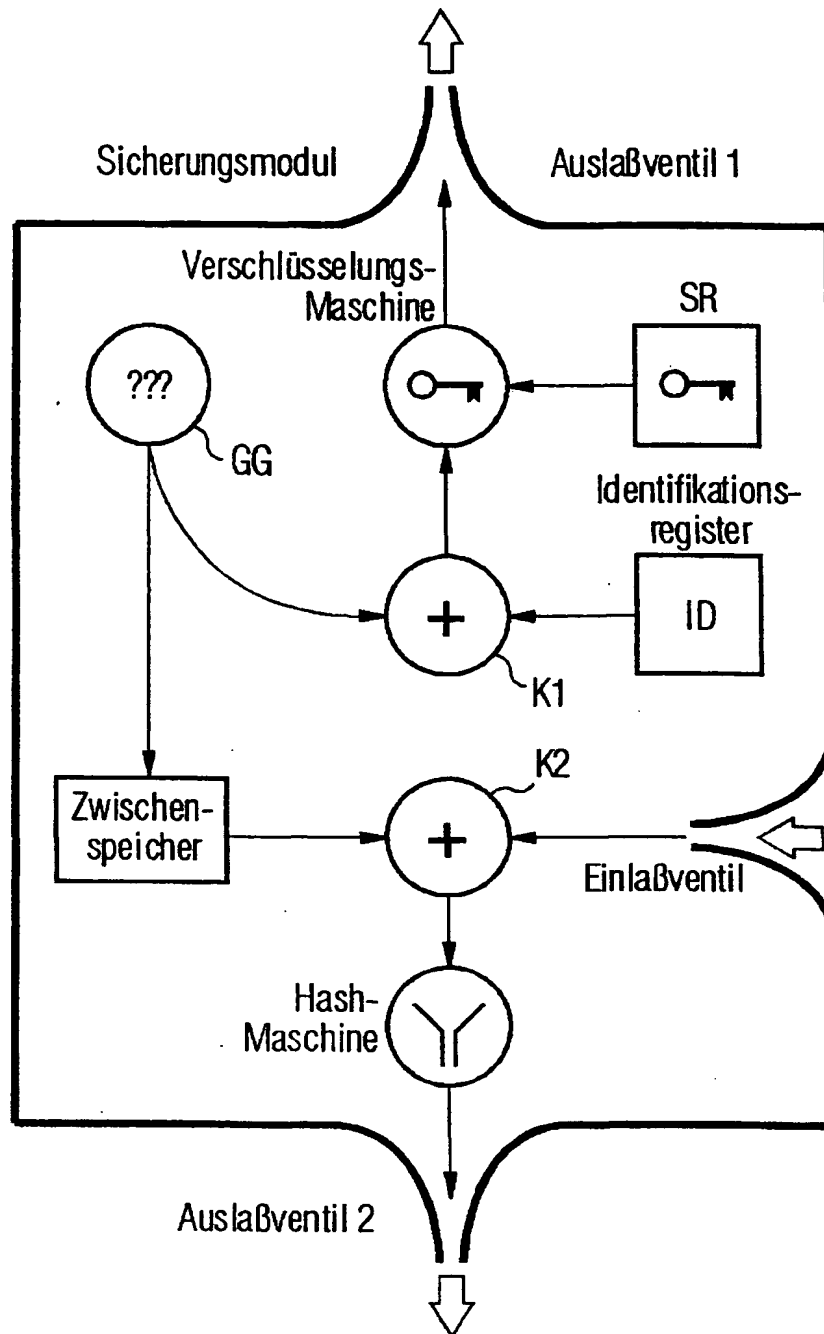
7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass durch den Vergleich ermittelt wird, ob in das Dokument von dem Dokumenthersteller eingebrachte Daten verfälscht wurden.

8. Verfahren zur Erstellung und zur späteren Überprüfung von fälschungssicheren Dokumenten, dadurch gekennzeichnet, dass die Dokumente in einem Verfahren nach einem oder mehreren der Ansprüche 1 bis 4 erzeugt werden und dass die Dokumente anschließend nach einem Verfahren nach einem oder mehreren der Ansprüche 5 bis 7 überprüft werden.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen der Bescheinigungs- und der Prüfstelle stattfindet.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -



Verfahren und System zur Erstellung fälschungssicherer Dokumente
Zeichnung 2

